UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/735,087	12/11/2000	David Michael Kurn	20206-033 (P00-3017)	5325

7590 01/26/2005

Hewlett-Packard Company
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
SON, LINH L D	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 01/26/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/735,087	KURN ET AL.	
	Examiner	Art Unit	
	Linh Son	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 December 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12,14-27 and 29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12,14-27 and 29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is a non-final action.

2. This Action is written in responding to the Amendment received on October 13, 2004.

3. Claims 1 to 12, 14 to 27, and 29 are pending. Claims 13 and 28 are canceled.

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-6,9-12, 14-21, 24-27, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Puhl et al, US Patent No 6223291B1, hereinafter "Puhl", in view of Yu et al, US Patent No 6067621, hereinafter "Yu".

7. As per claims 1 and 16, Puhl teaches "A cryptographic system, comprising: a database, the database configured to contain sensitive information (Member directory); at least one process; two or more master keys of which at least one master key is a

most-secure master key and requiring a multi-part construction to be exposed (encryption/decryption key (e/d key)), relative to the at least one most-secure master key each of the remaining one or more master keys is a less-secure master key (Member key), the at least one most-secure master key can be used for detecting tampering of any less-secure master key; and means for cryptographically linking one or more of the at least one most-secure master key with one or more less-secure master keys such that any tampering of the one or more less-secure master keys can be detected (e/d key = (Hash of ((member key)$_{Epassphrase}$, secret value))) (The hash is the linking mechanism and since the member key is included in the e/d key, the e/d key can be used to verify the member key)" in (Col 17 lines 25-40). However, Puhl does not specifically teach the composition of fewer parts to be exposed in generating of the less-secure master key. Nevertheless, Yu includes this feature completely in the process of generating a member key or client key with a composition of multiple parts in (Col 6 lines 40-67 to Col 7 lines 1-11). Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Puhl's invention to include Yu's multi-part client key generation to further enhancing the security level of the client key.

8. As per claims 2 and 17, Puhl teaches "A cryptographic system as in claim 1, wherein the cryptographic linking is performed by creating a message digest of the one or more most-secure master keys concatenated with the one or more less-secure

master keys, and saving the result in the database" in (Col 17 lines 25-40).

9. As per claims 3, and 18, Puhl teaches "A cryptographic system as in claim 1, wherein the cryptographic linking is performed by creating a message digest of the one or more most-secure master keys concatenated with a random value and further concatenated with the one or more less-secure master keys, and saving the result in a database" in (Col 17 lines 25-40).

10. As per claims 4 and 19, "A cryptographic system as in claim 3, wherein the random value is a Salt" is well know in that art.

11. As per claims 5 and 20, Puhl teaches method of generating a linking between two keys. However, Puhl does not teach "the use of the most-secure master key as a symmetric encryption key, to compute a symmetric message authentication code, and retaining some or all of the result". Nevertheless, Yu does teach this feature in (Col 6 lines 47-67). Therefore, it would be obvious at the time of the invention to modify Puhl's invention to include this feature to verify the authenticity of the message.

12. As per claims 6 and 21, Claim 5's rejection is incorporated. However, neither Puhl nor Yu teach an 8-byte result to compute the symmetric message authentication code, and only retaining 4-byte result. Nevertheless, Yu does teach a format converter to change the format of the password from binary to decimal number. Therefore, it

would be obvious at the time of the invention was made for one having ordinary skill in the art to modify the invention to generate the result in 8-byte and 4-byte. The motivation would reduce the storage space and the burden on the communication channel.

13. As per claims 9 and 24, Puhl teaches "A cryptographic system as in claims 1 and 16, wherein the two or more master keys are kept in non-swappable physical memory" in (Col 4 lines 47-54).

14. As per claims 10 and 25, Puhl teaches "A cryptographic system as in claims 9 and 24, wherein the non-swappable physical memory is protected" in (Col 4lines 47-54).

15. As per claims 11 and 26, Puhl teaches "A cryptographic system as in claim 1, wherein the two or more master keys are kept in virtual memory" in (Col 4lines 47-54).

16. As per claims 12 and 27, Puhl teaches "A cryptographic system as in claim 1, wherein, respectively, the at least one most-secure master key and the one or more less-secure master keys, include a protection key and an integrity key, the protection key protecting access to sensitive information and the integrity key ensuring the integrity of the sensitive information" in (Col 17 lines 25-40).

17. As per claims 14 and 29, Puhl teaches "A cryptographic system as in claim 1, wherein the sensitive information can be a public key" in (Col 17 lines 25-40).

18. As per claim 15, Puhl teaches "A cryptographic system as in claim 1, wherein the means for cryptographically linking is a key repository process for enforcing enterprise policies and policy decisions" in (Col 17 lines 25-40).

19. Claims 7-8, and 22-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Puhl in view of Matyas et al, US Patent No. 4941176.

20. As per claims 7 and 22, Puhl discloses a cryptographic system as in claims 6 and 16. However, Puhl do not teach the use of Cipher-block chaining (CBC) method to compute the symmetric message authentication code. Nevertheless, Matyas et al do implement the CBC in the "Secure Management of Keys using Control Vectors" invention (Col 45 lines 8-17). Therefor, it would be obvious at the time of the invention was made for one having ordinary skill in the art to use the same algorithm operation to ensure the data correction for the MAC.

21. As per claims 8 and 23, Puhl and Matyas et al disclose a cryptographic system as in claims 7 and 16, wherein the CBC is performed using a random number as an initialization vector, and wherein the initialization vector is saved along with the result (Matyas et al, Col 125 line 18).

Conclusion

1. Any inquiry concerning this communication from the examiner should be directed to Linh Son whose telephone number is (571)-271-3856.

2. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor Kim Y. Vu can be reached at (571)-272-3859. The fax numbers for this group are (703)-872-9306 (official fax). Any inquiry of general nature or relating to the status of this application or proceeding should be directed to the group receptionist whose telephone number is (571)-272-2100.

3. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval IPAIR.I system. Status information for published applications may be obtained from either Private PMR or Public PMR. Status information for unpublished applications is available through Private PMR only. For more information about the PAIR system, see http://pzr-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Linh LD Son

Patent Examiner

AU 2135